

T S7/5/1

7/5/1

DIALOG(R)File 351:Derwent WPI
(c) 2005 Thomson Derwent. All rts. reserv.

013608276

WPI Acc No: 2001-092484/200111

XRPX Acc No: N01-069981

**Electronic storage device for guaranteeing originality of electronic data
varies level of access based on if data are original data or not**

Patent Assignee: RICOH KK (RICO)

Inventor: KANAI Y; YACHIDA M

Number of Countries: 002 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111 B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340
A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A
19991129; JP 200015091 A 20000124

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1	159		G06F-012/14	
JP 2000339223	A	29		G06F-012/14	
JP 2001005728	A	46		G06F-012/14	
JP 2001147898	A	11		G06F-015/00	
JP 2001154577	A	12		G09C-001/00	
JP 2001209582	A	18		G06F-012/14	
JP 2001209581	A	16		G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74

Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA

Derwent Class: P85; T01

International Patent Class (Main): G06F-012/14; G06F-015/00

International Patent Class (Additional): G06F-003/06; G06F-009/06;
G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00

File Segment: EPI; EngPI

?

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2001-209582
(P2001-209582A)

(43)公開日 平成13年8月3日(2001.8.3)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 Z 5 B 0 1 7

審査請求 未請求 請求項の数21 O L (全 18 頁)

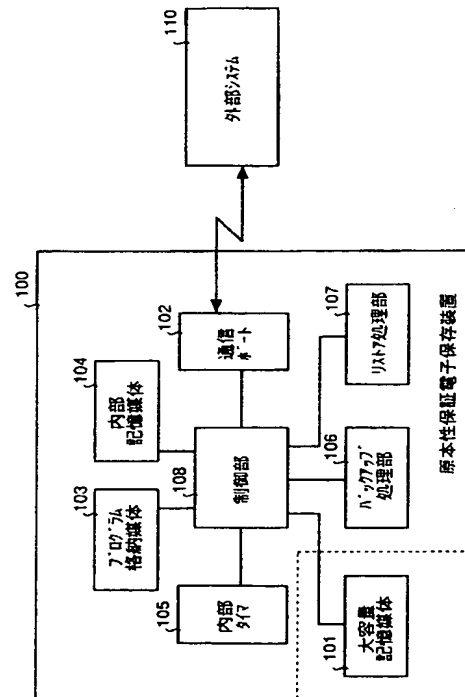
(21)出願番号	特願2000-15092(P2000-15092)	(71)出願人	000006747 株式会社リコー 東京都大田区中馬込1丁目3番6号
(22)出願日	平成12年1月24日(2000.1.24)	(72)発明者	金井 洋一 東京都大田区中馬込1丁目3番6号 株式 会社リコー内
		(72)発明者	谷内田 益義 東京都大田区中馬込1丁目3番6号 株式 会社リコー内
		(74)代理人	100104190 弁理士 酒井 昭徳 Fターム(参考) 5B017 AA05 BA07 CA16

(54)【発明の名称】 原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】 なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証すること。

【解決手段】 外部システム110からバックアップ要求を受け付けた際に、バックアップ処理手段106が、内部記憶媒体104に格納した管理情報についてのバックアップを作成し、また、外部システム110からリストア要求を受け付けた際に、リストア処理部107が、バックアップ処理部106によって生成されたバックアップ情報を内部記憶媒体104にリストアする。



【特許請求の範囲】

【請求項1】 内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置において、前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成手段と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成手段により生成されたバックアップ情報を前記内部記憶媒体にリストアするリストア手段と、

を備えたことを特徴とする原本性保証電子保存装置。

【請求項2】 前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする請求項1に記載の原本性保証電子保存装置。

【請求項3】 前記リストア手段は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする請求項2に記載の原本性保証電子保存装置。

【請求項4】 前記バックアップ情報生成手段は、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする請求項2または3に記載の原本性保証電子保存装置。

【請求項5】 前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第1の暗号化手段と、前記第1の暗号化手段による暗号化に用いた前記乱数を前記第1の暗号鍵により暗号化する第2の暗号化手段と、前記第1の暗号化手段により暗号化された暗号化管理情報および前記第2の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力手段と、を備えたことを特徴とする請求項1に記載の原本性保証電子保存装置。

【請求項6】 前記リストア手段は、前記バックアップ情報に含まれる暗号化乱数を前記第1の復号鍵で復号化する第1の復号化手段と、前記第1の復号化手段により復号化された乱数で前記暗号化管理情報を復号化する第2の復号化手段と、前記第2の復号化手段により復号化された管理情報を前記内部記憶媒体に記録する記録手段と、を備えたことを特徴とする請求項5に記載の原本性保証

電子保存装置。

【請求項7】 前記出力手段は、前記第1の暗号化手段により暗号化された暗号化管理情報に前記第2の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成手段と、前記暗号化内部情報作成手段により作成された暗号化内部情報のハッシュ値を算定する第1のハッシュ値算定手段とを備え、

前記ハッシュ値算定手段により算定されたハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする請求項5に記載の原本性保証電子保存装置。

【請求項8】 前記リストア手段は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第2のハッシュ値算定手段と、前記第2のハッシュ値算定手段により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較手段と、

前記比較手段により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第1の暗号鍵に対応する第1の復号鍵で復号化する第1の復号化手段と、前記第1の復号化手段により復号化された乱数を用いて前記暗号化管理情報を復号化する第2の復号化手段と、を備えたことを特徴とする請求項7に記載の原本性保証電子保存装置。

【請求項9】 前記出力手段は、前記ハッシュ値算定手段により算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力し、前記比較手段は、前記第2の暗号鍵に対応する第2の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第2のハッシュ値算定手段により算定されたハッシュ値とを比較することを特徴とする請求項8に記載の原本性保証電子保存装置。

【請求項10】 前記第1の暗号鍵および前記第2の復号鍵は公開鍵暗号系の公開鍵であり、前記第2の暗号鍵および前記第1の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする請求項9に記載の原本性保証電子保存装置。

【請求項11】 内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置の障害復旧方法において、前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成工程と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成工程により生成されたバックアップ情報を前記内部記憶媒体にリストアするリス

トア工程と、
を含んだことを特徴とする障害復旧方法。

【請求項12】 前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする請求項11に記載の障害復旧方法。

【請求項13】 前記リストア工程は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする請求項12に記載の障害復旧方法。

【請求項14】 前記バックアップ情報生成工程は、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする請求項12または13に記載の障害復旧方法。

【請求項15】 前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第1の暗号化工程と、前記第1の暗号化工程による暗号化に用いた前記乱数を前記第1の暗号鍵により暗号化する第2の暗号化工程と、前記第1の暗号化工程により暗号化された暗号化管理情報および前記第2の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力工程と、を含んだことを特徴とする請求項11に記載の障害復旧方法。

【請求項16】 前記リストア工程は、前記バックアップ情報に含まれる暗号化乱数を前記第1の復号鍵で復号化する第1の復号化工程と、前記第1の復号化工程により復号化された乱数で前記暗号化管理情報を復号化する第2の復号化工程と、前記第2の復号化工程により復号化された管理情報を前記内部記憶媒体に記録する記録工程と、を含んだことを特徴とする請求項15に記載の障害復旧方法。

【請求項17】 前記出力工程は、前記第1の暗号化工程により暗号化された暗号化管理情報に前記第2の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成工程と、前記暗号化内部情報作成工程により作成された暗号化内部情報のハッシュ値を算定する第1のハッシュ値算定工程とを含み、前記ハッシュ値算定工程により算定されたハッシュ値を

前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする請求項15に記載の障害復旧方法。

【請求項18】 前記リストア工程は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第2のハッシュ値算定工程と、前記第2のハッシュ値算定工程により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較工程と、

10 前記比較工程により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第1の暗号鍵に対応する第1の復号鍵で復号化する第1の復号化工程と、前記第1の復号化工程により復号化された乱数を用いて前記暗号化管理情報を復号化する第2の復号化工程と、を含んだことを特徴とする請求項17に記載の障害復旧方法。

【請求項19】 前記出力工程は、前記ハッシュ値算定工程により算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力し、

20 前記比較工程は、前記第2の暗号鍵に対応する第2の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第2のハッシュ値算定工程により算定されたハッシュ値とを比較することを特徴とする請求項18に記載の障害復旧方法。

【請求項20】 前記第1の暗号鍵および前記第2の復号鍵は公開鍵暗号系の公開鍵であり、前記第2の暗号鍵および前記第1の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする請求項19に記載の障害復旧方法。

【請求項21】 前記請求項11～20のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置、障害復旧方法および記録媒体に関する。

【0002】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類とし

て保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【0003】たとえば、「金井他：原本性保証電子保存システムの開発—システムの構築—, Medical Imaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発, (特)情報処理振興事業協会発行 創造的ソフトウェア育成事業およびエレクトロニック・コマース推進事業 最終成果発表会論文集 創造的ソフトウェア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【0004】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【0005】

【発明が解決しようとする課題】しかしながら、これらの従来技術は、原本となる電子データを格納する大容量記憶媒体以外は、あるレベルの耐タンパー性を持った筐体に格納されていることを前提とするため、原本性保証電子保存装置になんらかの障害が生じた場合に、その障害対処に時間を要する。

【0006】具体的には、電子データの原本性を保証するためには、内部記憶媒体に記憶した内部管理情報を通常利用することとなるが、この内部記憶媒体に記憶した内部管理情報が障害などによって失われると、耐タンパー性が保持されているためにかえってその復旧に時間を要する結果となる。

【0007】このため、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置をいかに実現するかが極めて重要な課題となっている。

【0008】この発明は、上記問題(課題)に鑑みてなされたものであり、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するため、請求項1に記載の発明にかかる原本性保証電子保存装置は、内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置において、前記内部記憶媒体に格納した管理情報のバックアップ情報を生成する

バックアップ情報生成手段と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成手段により生成されたバックアップ情報を前記内部記憶媒体にリストアするリストア手段と、を備えたことを特徴とする。

【0010】この請求項1に記載の発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる。

【0011】また、請求項2に記載の発明にかかる原本性保証電子保存装置は、前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする。

【0012】この請求項2に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる。

【0013】また、請求項3に記載の発明にかかる原本性保証電子保存装置は、前記リストア手段は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする。

【0014】この請求項3に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録することとしたので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる。

【0015】また、請求項4に記載の発明にかかる原本性保証電子保存装置は、前記バックアップ情報生成手段は、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする。

【0016】この請求項4に記載の発明によれば、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いてバックアップ情報の作成または復号をおこなうこととしたので、ICカードに応じて暗号鍵および復号鍵を自在に変更することができる。

【0017】また、請求項5に記載の発明にかかる原本性保証電子保存装置は、前記バックアップ情報生成手段は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第1の暗号化手段と、前記第1の暗号化手段による暗号化に用いた前記乱数を前記第1の暗号鍵により暗号化する第2の暗号化手段と、前記第1の暗号化手段により暗号化された暗号化管理情報および前記第2の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力手段と、を備えたことを特徴とする。

【0018】この請求項5に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第1の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力することとしたので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる。

【0019】また、請求項6に記載の発明にかかる原本性保証電子保存装置は、前記リストア手段は、前記バックアップ情報に含まれる暗号化乱数を前記第1の復号鍵で復号化する第1の復号化手段と、前記第1の復号化手段により復号化された乱数で前記暗号化管理情報を復号化する第2の復号化手段と、前記第2の復号化手段により復号化された管理情報を前記内部記憶媒体に記録する記録手段と、を備えたことを特徴とする。

【0020】この請求項6に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第1の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録することとしたので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる。

【0021】また、請求項7に記載の発明にかかる原本性保証電子保存装置は、前記出力手段は、前記第1の暗号化手段により暗号化された暗号化管理情報に前記第2の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成手段と、前記暗号化内部情報作成手段により作成された暗号化内部情報のハッシュ値を算定する第1のハッシュ値算定手段とを備え、前記ハッシュ値算定手段により算定されたハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする。

【0022】この請求項7に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力することとしたので、暗号化内部情報の改ざんを効率良く防止することができ

る。

【0023】また、請求項8に記載の発明にかかる原本性保証電子保存装置は、前記リストア手段は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第2のハッシュ値算定手段と、前記第2のハッシュ値算定手段により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較手段と、前記比較手段により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第1の暗号鍵に対応する第1の復号鍵で復号化する第1の復号化手段と、前記第1の復号化手段により復号化された乱数を用いて前記暗号化管理情報を復号化する第2の復号化手段と、を備えたことを特徴とする。

【0024】この請求項8に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化することとしたので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる。

【0025】また、請求項9に記載の発明にかかる原本性保証電子保存装置は、前記出力手段は、前記ハッシュ値算定手段により算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成手段により作成された暗号化内部情報とともに前記バックアップ情報として出力し、前記比較手段は、前記第2の暗号鍵に対応する第2の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第2のハッシュ値算定手段により算定されたハッシュ値とを比較することを特徴とする。

【0026】この請求項9に記載の発明によれば、算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第2の暗号鍵に対応する第2の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較することとしたので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる。

【0027】また、請求項10に記載の発明にかかる原本性保証電子保存装置は、前記第1の暗号鍵および前記第2の復号鍵は公開鍵暗号系の公開鍵であり、前記第2の暗号鍵および前記第1の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする。

【0028】この請求項10に記載の発明によれば、第1の暗号鍵および第2の復号鍵を公開鍵暗号系の公開鍵とし、第2の暗号鍵および第1の復号鍵を公開鍵暗号系の秘密鍵としたので、公開鍵暗号系を用いてバックアップ

ブ情報の暗号強度を高めることができる。

【0029】また、請求項11に記載の発明にかかる障害復旧方法は、内部記憶媒体に格納した所定の管理情報に基づいて大容量記憶媒体に格納した保存データの原本性を保証する原本性保証電子保存装置の障害復旧方法において、前記内部記憶媒体に格納した管理情報のバックアップ情報を生成するバックアップ情報生成工程と、前記内部記憶媒体に格納した管理情報を喪失した場合に、前記バックアップ情報生成工程により生成されたバックアップ情報を前記内部記憶媒体にリストアするリストア工程と、を含んだことを特徴とする。

【0030】この請求項11に記載の発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる。

【0031】また、請求項12に記載の発明にかかる障害復旧方法は、前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することを特徴とする。

【0032】この請求項12に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる。

【0033】また、請求項13に記載の発明にかかる障害復旧方法は、前記リストア工程は、前記バックアップ情報とともにリストア要求を前記外部システムから受け付けた際に、前記バックアップ情報を前記第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として前記内部記憶媒体に記録することを特徴とする。

【0034】この請求項13に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録することとしたので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる。

【0035】また、請求項14に記載の発明にかかる障害復旧方法は、前記バックアップ情報生成工程は、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いて前記バックアップ情報の作成または復号をおこなうことを特徴とする。

【0036】この請求項14に記載の発明によれば、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いてバックアップ情報の作成または復号をおこなうこととしたので、ICカードに応じて暗号鍵および復号鍵を自在に変更することができる。

【0037】また、請求項15に記載の発明にかかる障害復旧方法は、前記バックアップ情報生成工程は、外部システムからバックアップ要求を受け付けた場合に、前記内部記憶媒体に格納した管理情報を所定の乱数により暗号化する第1の暗号化工程と、前記第1の暗号化工程による暗号化に用いた前記乱数を前記第1の暗号鍵により暗号化する第2の暗号化工程と、前記第1の暗号化工程により暗号化された暗号化管理情報および前記第2の暗号化手段により暗号化された暗号化乱数を前記バックアップ情報として出力する出力工程と、を含んだことを特徴とする。

【0038】この請求項15に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第1の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力することとしたので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる。

【0039】また、請求項16に記載の発明にかかる障害復旧方法は、前記リストア工程は、前記バックアップ情報に含まれる暗号化乱数を前記第1の復号鍵で復号化する第1の復号化工程と、前記第1の復号化工程により復号化された乱数で前記暗号化管理情報を復号化する第2の復号化工程と、前記第2の復号化工程により復号化された管理情報を前記内部記憶媒体に記録する記録工程と、を含んだことを特徴とする。

【0040】この請求項16に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第1の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録することとしたので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる。

【0041】また、請求項17に記載の発明にかかる障害復旧方法は、前記出力工程は、前記第1の暗号化工程により暗号化された暗号化管理情報に前記第2の暗号化手段により暗号化された暗号化乱数を付与して暗号化内部情報を作成する暗号化内部情報作成工程と、前記暗号化内部情報作成工程により作成された暗号化内部情報のハッシュ値を算定する第1のハッシュ値算定工程とを含み、前記ハッシュ値算定工程により算定されたハッシュ値を前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力することを特徴とする。

【0042】この請求項17に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力することとしたので、暗号化内部情報の改ざんを効率良く防止することができる。

【0043】また、請求項18に記載の発明にかかる障害復旧方法は、前記リストア工程は、前記バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定する第2のハッシュ値算定工程と、前記第2のハッシュ値算定工程により算定されたハッシュ値と前記バックアップ情報に含まれるハッシュ値とを比較する比較工程と、前記比較工程により両ハッシュ値が一致すると判断された場合に、前記暗号化乱数を前記第1の暗号鍵に対応する第1の復号鍵で復号化する第1の復号化工程と、前記第1の復号化工程により復号化された乱数を用いて前記暗号化管理情報を復号化する第2の復号化工程と、を含んだことを特徴とする。

【0044】この請求項18に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化することとしたので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる。

【0045】また、請求項19に記載の発明にかかる障害復旧方法は、前記出力工程は、前記ハッシュ値算定工程により算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を前記暗号化内部情報作成工程により作成された暗号化内部情報とともに前記バックアップ情報として出力し、前記比較工程は、前記第2の暗号鍵に対応する第2の復号鍵を用いて前記暗号化ハッシュ値を復号化したハッシュ値と前記第2のハッシュ値算定工程により算定されたハッシュ値とを比較することとを特徴とする。

【0046】この請求項19に記載の発明によれば、算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第2の暗号鍵に対応する第2の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較することとしたので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる。

【0047】また、請求項20に記載の発明にかかる障害復旧方法は、前記第1の暗号鍵および前記第2の復号鍵は公開鍵暗号系の公開鍵であり、前記第2の暗号鍵お

よび前記第1の復号鍵は前記公開鍵暗号系の秘密鍵であることを特徴とする。

【0048】この請求項20に記載の発明によれば、第1の暗号鍵および第2の復号鍵を公開鍵暗号系の公開鍵とし、第2の暗号鍵および第1の復号鍵を公開鍵暗号系の秘密鍵としたので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができる。

【0049】また、請求項21に記載の発明にかかる記録媒体は、前記請求項11～20のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項11～20の動作をコンピュータによって実現することができる。

【0050】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかる原本性保証電子保存装置、障害復旧方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0051】図1は、本実施の形態において用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示す原本性保証電子保存装置100は、原本の電子データを大容量記憶媒体101上に保持しておき、内部記憶媒体104に格納した管理情報などを用いてこの電子データの原本性を保証することようにした装置である。

【0052】ここで、この原本性保証電子保存装置100になんらかの障害が発生した場合には、内部記憶媒体104に格納した情報が失われてしまい、電子データの原本性を保証することができなくなる。特に、大容量記憶媒体101以外は耐タンパー性を持った筐体に格納されるため、管理情報を簡易に再設定することは難しい。

【0053】このため、この原本性保証電子保存装置100では、内部記憶媒体104に格納した管理情報をバックアップするとともに、この原本性保証電子保存装置100になんらかの障害が発生した場合には、バックアップした管理情報を内部記憶媒体104にリストアするよう構成している。

【0054】ただし、かかる管理情報は、そもそも原本となる電子データの原本性を保証するために用いるものであり、むやみに装置外部に保持すべきものではないので、その暗号強度を高めることで、本来の原本性保証に影響を与えないようにしている。

【0055】同図に示すように、この原本性保証電子保存装置100は、大容量記憶媒体101と、通信ポート102と、プログラム格納媒体103と、内部記憶媒体104と、内部タイマ105と、バックアップ処理部106と、リストア処理部107と、制御部108とからなる。

【0056】大容量記憶媒体101は、原本となる電子

データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやCD-Rなどからなる。この大容量記憶媒体101は、図中に破線で示したように原本性保証電子保存装置100から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置100と物理的に一体化し、通信ポート102以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【0057】ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【0058】通信ポート102は、ネットワークを介して外部システム110との通信をおこなうためのインターフェース部であり、たとえばLANカードなどの通信モデムなどからなる。

【0059】プログラム格納媒体103は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なEEPROMや読み出し専用のROMなどからなる。

【0060】内部記憶媒体104は、各種プログラムの実行に必要なパラメータを記憶するEEPROMなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。内部タイマ105は、制御部108の本体をなすプロセッサがプログラムの実行時に所得する時刻を計時するタイマである。

【0061】バックアップ処理部106は、乱数および公開鍵などを用いて内部記憶媒体104に格納した管理情報のバックアップ情報を生成する処理部であり、具体的には、内部記憶媒体104から装置設定ファイルなどの後述する各種ファイルを読み出して内部管理情報一括データとする。その後、装置内部で乱数を生成してこの乱数を公開鍵で暗号化して、暗号化乱数を作成するとともに、該乱数で内部管理情報一括データを一括して暗号化し、これに暗号化乱数を付与して内部管理情報一括暗号化データとする。

【0062】その後、この内部管理情報一括暗号化データについてのハッシュ値を計算し、このハッシュ値を秘密鍵で暗号化してプログラム署名を作成し、このプログラム署名を内部管理情報一括暗号化データに付与して、内部管理情報一括パッケージデータを作成して、外部システム110に送出する。

【0063】リストア処理部107は、内部記憶媒体104に格納した管理情報を喪失した場合に、バックアップ処理部106により生成されたバックアップ情報に含まれる管理情報を内部記憶媒体104にリストアする処

理部である。

【0064】具体的には、外部システム110から内部管理情報一括パッケージデータを受け取ったならば、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し、内部管理情報一括暗号化データのハッシュ値を計算するとともに、プログラム署名を公開鍵で復号化する。

【0065】そして、両ハッシュ値が一致する場合には、内部管理情報一括暗号化データに含まれる暗号化乱数を秘密鍵で復号化して乱数を取得し、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し、この内部管理情報一括データを形成する各ファイルを内部記憶媒体104に格納する。

【0066】制御部108は、その実体はプロセッサであり、プログラム格納媒体103に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラム、復号化プログラムおよびバックアップ制御プログラムなどの各種プログラムを読み出して実行することになる。

【0067】具体的には、この制御部108では、外部システム110などから内部管理情報のバックアップ作成要求を受け付けた際に、バックアップの作成をバックアップ106に対して指示するとともに、外部システム110などからリストア要求を受け付けた際に、リストア処理部107に対してリストア指示をおこなう。

【0068】なお、本実施の形態では、説明の便宜上外部システム110などからの要求に応答してバックアップ並びにリストアをおこなうよう制御することとしたが、内部タイマ105の計時に基づいて定期的にバックアップ指示をおこなうとともに、内部記憶媒体104の異常を検知してリストア指示をおこなうよう構成することもできる。

【0069】上記構成を有する原本性保証電子保存装置100を用いることにより、内部記憶媒体104に格納した管理情報を効率良くバックアップするとともに、状況に応じてバックアップ情報を内部記憶媒体104に迅速にリストアし、もって大容量記憶媒体101に格納した原本の電子データの原本性を継続的に保証することができる。

【0070】つぎに、図1に示した大容量記憶媒体101に保持したファイル並びに内部記憶媒体104に保持したファイルについて説明する。図2は、図1に示した大容量記憶媒体101上に保持した電子データ並びに内部記憶媒体104に保持した管理情報を説明するための説明図である。

【0071】同図に示すように、大容量記憶媒体101には、原本としての各電子データが保存データとして格納されるとともに、その保存データを管理するための保存データリストファイルと、媒体ごとに管理するための媒体管理情報ファイルが格納されている。

【0072】具体的には、この保存データリストファイルは、保存データごとに設けられた複数の保存データエントリからなり、各保存データエントリは、保存データ識別番号、保存データ名、作成情報、最終更新情報、廃棄情報および最新のバージョン番号などで形成される。また、媒体管理情報ファイルは、媒体識別番号、媒体名および媒体初期化日時情報などで形成される。

【0073】これに対して、内部記憶媒体104には、電子署名の計算などに使用する装置固有の装置暗号鍵（公開鍵暗号系の場合には秘密鍵）、電子署名の検証などに用いる装置固有の装置復号鍵（公開鍵暗号系の場合には公開鍵）、保存データ識別番号や媒体識別番号を生成する際に用いる装置識別番号、つぎの保存データに付与する保存データ識別番号、つぎにフォーマットする媒体に付与するつぎの媒体識別番号、大容量記憶媒体101の真正性を検証するための媒体認証コードリスト、内部タイマ設定履歴、外部システム110のアカウントを管理するアカウント管理リスト並びに装置アクセスログなどを格納する。

【0074】具体的には、図中に示した装置設定ファイルには、上記装置暗号鍵、装置復号鍵、装置識別情報、つぎの保存データ識別番号およびつぎの媒体識別番号などが記録され、また、媒体認証コードリストファイルには、媒体識別番号および媒体認証コードなどが記録される。さらに、内部タイマ設定履歴ファイルには内部タイマ設定履歴が記録され、装置アクセス履歴ファイルには装置アクセス履歴が記録され、アカウント管理リストファイルにはアカウント管理リストが記録されている。

【0075】つぎに、図1に示した外部システム110からの原本性保証電子保存装置100へのログイン手順について説明する。図3は、図1に示した外部システム110からの原本性保証電子保存装置100へのログイン手順を示すフローチャートである。

【0076】まず、内部管理情報のバックアップをおこなう際には、管理者などが外部システム110を用いて原本性保証電子保存装置100に対してログインをしなければならない。なお、ここではパスワードによる一般的なチャレンジレスポンス認証処理をおこなうこととする。

【0077】同図に示すように、外部システム110が、原本性電子保存装置100に対してアカウント名とログイン要求を送信すると（ステップS301）、原本性保証電子保存装置100は、このアカウント名とログイン要求を受信し（ステップS302）、内部記憶媒体104からアカウント管理テーブルを取得し（ステップS303）、このアカウント管理テーブルから該当するアカウントエントリを取得する（ステップS304）。

【0078】そして、該当するエントリが存在するか否かを確認し（ステップS305）、該当するエントリが存在しない場合（ステップS305否定）は、エラーの

終了コードを外部システム110のクライアントに送信し（ステップS306）、エラー処理をおこなって（ステップS318）、処理を終了する。

【0079】これに対して、該当するエントリが存在する場合（ステップS305肯定）は、乱数を生成し（ステップS307）、この乱数を外部システム110のクライアントに送信するとともに（ステップS308）、該乱数とアカウントエントリに格納されているユーザ側内部認証鍵を合わせたものに対してハッシュ値を計算する（ステップS309）。

【0080】また、外部システム110がこの乱数を受信したならば（ステップS310）、この乱数とパスワードを合わせたものに対してハッシュ値を計算し（ステップS311）、計算したハッシュ値を原本性保証電子保存装置100に対して送信する（ステップS312）。

【0081】そして、原本性保証電子保存装置100が、このハッシュ値を受信すると（ステップS313）、受信したハッシュ値が計算したハッシュ値と一致するか否かを確認し（ステップS314）、両者が一致しない場合（ステップS314否定）は、エラーの結果コードをクライアントに送信し（ステップS315）、エラー処理をおこなって（ステップS318）、処理を終了する。

【0082】一方、両者が一致する場合（ステップS314肯定）には、成功した結果コードを外部システム110のクライアントに送信し（ステップS316）、ログインしたアカウントのアカウントエントリを内部に保持する（ステップS317）。

【0083】なお、外部システム110が結果コードを受信したならば（ステップS319）、この結果コードがエラーコードであるか否かを確認し（ステップS320）、エラーコードである場合（ステップS320肯定）は、エラー処理をおこなう（ステップS321）。

【0084】上記一連の処理をおこなうことにより、外部システム110からクライアントがバックアップ要求をおこなうに際して、原本性保証電子保存装置100に対して正常にログインすることができる。

【0085】つぎに、図1に示したバックアップ処理部106などによるバックアップ手順について説明する。図4は、図1に示したバックアップ処理部106などによるバックアップ手順を示すフローチャートである。

【0086】同図に示すように、原本性保証電子保存装置100がバックアップ要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップS401）、装置管理者のアカウント権限があるか否かを確認する（ステップS402）。そして、アカウント権限がない場合（ステップS402否定）は、エラー処理をおこなった後に（ステップS412）、処理を終了する。

【0087】これに対して、アカウント権限がある場合（ステップS402肯定）は、内部記憶媒体104から装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルを読み出し（ステップS403）、読み出したファイルを一括して内部管理情報一括データとする（ステップS404）。

【0088】なお、内部記憶媒体104に記憶する装置アクセス履歴ファイルについては、外部システム110から原本性保証電子保存装置100へのアクセスが生ずるたびに頻繁に変更されるファイルであるため、ここではこの装置アクセス履歴ファイルのバックアップはおこなわないものとする。

【0089】その後、装置内部で乱数を生成し（ステップS405）、この乱数をプログラム内部のプログラム公開鍵で暗号化して暗号化乱数を作成し（ステップS406）、該乱数により内部管理情報一括データを暗号化し、これに暗号化乱数を付与して内部管理情報一括暗号化データとする（ステップS407）。

【0090】その後、この内部管理情報一括暗号化データについてのハッシュ値を計算し（ステップS408）、このハッシュ値を秘密鍵で暗号化してプログラム署名を作成し（ステップS409）、このプログラム署名を内部管理情報一括暗号化データに付与して、内部管理情報一括パッケージデータを作成して（ステップS410）、外部システム110に送出する（ステップS411）。

【0091】つぎに、図1に示したリストア処理部107などによるリストア手順について説明する。図5は、図1に示したリストア処理部107などによるリストア手順を示すフローチャートである。なお、ここでは全く新しい原本性保証電子保存装置100に内部管理情報をリストアする場合を示すこととする。

【0092】同図に示すように、原本性保証電子保存装置100がリストア要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップS501）、装置管理者のアカウント権限があるか否かを確認する（ステップS502）。そして、アカウント権限がない場合（ステップS502否定）は、エラー処理をおこなった後に（ステップS517）、すべての処理を終了する。

【0093】これに対して、アカウント権限がある場合（ステップS502肯定）は、完全に新しい原本性保証電子保存装置100であるか否かについても確認し（ステップS503）、新しい原本性保証電子保存装置100でない場合（ステップS503否定）は、エラー処理をおこなった後に（ステップS517）、すべての処理を終了する。

【0094】一方、新しい原本性保証電子保存装置100である場合（ステップS503肯定）は、外部システ

ム110から内部管理情報一括パッケージデータを受け取り（ステップS504）、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し（ステップS505）、内部管理情報一括暗号化データのハッシュ値を計算するとともに（ステップS506）、プログラム署名をプログラム内部に保持しているプログラム公開鍵で復号化する（ステップS507）。

【0095】そして、復号化したものが先のハッシュ値と一致するか否かを確認し（ステップS508）、両ハッシュ値が一致しない場合（ステップS508否定）には、エラー処理をおこない（ステップS517）、その後、すべての処理を終了する。

【0096】これに対して、両ハッシュ値が一致する場合（ステップS508肯定）は、内部管理情報一括暗号化データから暗号化乱数を取得し（ステップS509）、この暗号化乱数をプログラム内部に保持しているプログラム秘密鍵で復号化して乱数を取得し（ステップS510）、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し（ステップS511）、この内部管理情報一括データを分解して、装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルとして内部記憶媒体104に記録する（ステップS512）。

【0097】そして、外部システム110から受け取った現在時刻で内部タイマ105を設定し（ステップS513）、設定前の日時情報を不明とし、設定後の日時情報を先に受け取った現在時刻に設定したタイマ設定エントリを作成する（ステップS514）。そして、内部設定履歴ファイルに新しいタイマ設定エントリを追加し（ステップS515）、装置アクセス履歴ファイルに、リストアしたことを示すログを記録して（ステップS516）、処理を終了する。

【0098】ところで、上記処理では、全く新しい原本性保証電子保存装置100に内部管理情報をリストアすることとしたが、すでに使用している原本性保証電子保存装置100に相乗りする形で内部管理情報をリストアする場合もある。

【0099】そこで、つぎに、使用している原本性保証電子保存装置100に相乗りする形で内部管理情報をリストアする場合のリストア手順について説明する。図6は、図1に示したリストア処理部107などが、使用している原本性保証電子保存装置100に相乗りする形で内部管理情報をリストアする場合のリストア手順を示すフローチャートである。

【0100】同図に示すように、この場合にも、原本性保証電子保存装置100がリストア要求を受け付けたならば、内部に保持しているアカウントエントリのアカウント権限を参照し（ステップS601）、装置管理者の

アカウント権限があるか否かを確認する（ステップS 6 0 2）。そして、アカウント権限がない場合（ステップS 6 0 2 否定）は、エラー処理をおこなった後に（ステップS 6 1 6）、処理を終了する。

【0101】これに対して、アカウント権限がある場合（ステップS 6 0 2 肯定）は、外部システム110から内部管理情報一括パッケージデータを受け取り（ステップS 6 0 3）、この内部管理情報一括パッケージデータを内部管理情報一括暗号化データとプログラム署名とに分離し（ステップS 6 0 4）、内部管理情報一括暗号化データのハッシュ値を計算するとともに（ステップS 6 0 5）、プログラム署名をプログラム内部に保持しているプログラム公開鍵で復号化する（ステップS 6 0 6）。

【0102】そして、復号化したものが先のハッシュ値と一致するか否かを確認し（ステップS 6 0 7）、両ハッシュ値が一致しない場合（ステップS 6 0 7 否定）には、エラー処理をおこなった後に（ステップS 6 1 6）、処理を終了する。

【0103】これに対して、両ハッシュ値が一致する場合（ステップS 6 0 7 肯定）は、内部管理情報一括暗号化データから暗号化乱数を取得し（ステップS 6 0 8）、この暗号化乱数をプログラム内部に保持しているプログラム秘密鍵で復号化して乱数を取得し（ステップS 6 0 9）、この乱数で内部管理情報一括暗号化データを復号化して内部管理情報一括データを取得し（ステップS 6 1 0）、この内部管理情報一括データを分解して（ステップS 6 1 1）、分解して得られた装置設定ファイルから装置識別番号を取得する（ステップS 6 1 2）。

【0104】そして、装置識別番号を名前とするフォルダを内部記憶媒体104に作成し（ステップS 6 1 3）、そのフォルダの下に、分解して得られた装置設定ファイル、媒体認証コードリストファイル、内部タイマ設定履歴ファイル、アカウント管理リストファイルとして内部記憶媒体104に記録するとともに（ステップS 6 1 4）、装置アクセス履歴ファイルに、リストアしたことを示すログを記録して（ステップS 6 1 5）、処理を終了する。

【0105】上述してきたように、本実施の形態にかかる原本性保証電子保存装置100では、外部システム110からバックアップ要求を受け付けた際に、バックアップ処理手段106が、内部記憶媒体104に格納した管理情報についてのバックアップを作成し、また、外部システム110からリストア要求を受け付けた際に、リストア処理部107が、バックアップ処理部106によって生成されたバックアップ情報を内部記憶媒体104にリストアするよう構成したので、内部記憶媒体104に格納した管理情報を効率良くバックアップするとともに、状況に応じてバックアップ情報を内部記憶媒体10

4に迅速にリストアし、もって大容量記憶媒体101に格納した原本の電子データの原本性を継続的に保証することができる。

【0106】なお、本実施の形態で説明した障害復旧方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーション等のコンピュータまたはマイコン内蔵のプリンタ、ディジタル複写機等で実行することにより実現される。このプログラムは、RAM、ROM、ハードディスク、フロッピーディスク、CD-ROM、MO、DVD等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介して、あるいは伝送媒体としてネットワークを介して配布することができる。

【0107】

【発明の効果】以上説明したように、請求項1に記載の発明によれば、内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアすることとしたので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる原本性保証電子保存装置が得られるという効果を奏する。

【0108】また、請求項2に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力することとしたので、バックアップ情報の暗号強度を高めることができる原本性保証電子保存装置が得られるという効果を奏する。

【0109】また、請求項3に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録するよう構成したので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる原本性保証電子保存装置が得られるという効果を奏する。

【0110】また、請求項4に記載の発明によれば、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いてバックアップ情報の作成または復号をおこなうよう構成したので、ICカードに応じて暗号鍵および復号鍵を自在に変更することができる原本性保証電子保存装置が得られるという効果を奏する。

【0111】また、請求項5に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、

内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第1の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力するよう構成したので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる原本性保証電子保存装置が得られるという効果を奏する。

【0112】また、請求項6に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第1の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録するよう構成したので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる原本性保証電子保存装置が得られるという効果を奏する。

【0113】また、請求項7に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力するよう構成したので、暗号化内部情報の改ざんを効率良く防止することができる原本性保証電子保存装置が得られるという効果を奏する。

【0114】また、請求項8に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化するよう構成したので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【0115】また、請求項9に記載の発明によれば、算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第2の暗号鍵に対応する第2の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較するよう構成したので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる原本性保証電子保存装置が得られるという効果を奏する。

【0116】また、請求項10に記載の発明によれば、第1の暗号鍵および第2の復号鍵を公開鍵暗号系の公開鍵とし、第2の暗号鍵および第1の復号鍵を公開鍵暗号系の秘密鍵とするよう構成したので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができる原本性保証電子保存装置が得られるという効果を奏する。

【0117】また、請求項11に記載の発明によれば、

内部記憶媒体に格納した管理情報のバックアップ情報を生成しておき、この内部記憶媒体に格納した管理情報を喪失した場合に、生成されたバックアップ情報を内部記憶媒体にリストアするよう構成したので、なんらかの障害が発生した場合であっても、内部記憶媒体に記憶した内部管理情報を迅速に復旧し、もって電子データの原本性を迅速かつ効率良く保証することができる障害復旧方法が得られるという効果を奏する。

【0118】また、請求項12に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を第1の暗号鍵で暗号化したバックアップ情報を作成し、作成したバックアップ情報を出力するよう構成したので、バックアップ情報の暗号強度を高めることができる障害復旧方法が得られるという効果を奏する。

【0119】また、請求項13に記載の発明によれば、バックアップ情報とともにリストア要求を外部システムから受け付けた際に、バックアップ情報を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化したバックアップ情報を管理情報として内部記憶媒体に記録するよう構成したので、暗号化されたバックアップ情報を正しく復号化して内部記憶媒体にリストアすることができる障害復旧方法が得られるという効果を奏する。

【0120】また、請求項14に記載の発明によれば、装置本体に装着したICカードの内部に保持した第1の暗号鍵および第1の復号鍵を用いてバックアップ情報の作成または復号をおこなうよう構成したので、ICカードに応じて暗号鍵および復号鍵を自在に変更することができる障害復旧方法が得られるという効果を奏する。

【0121】また、請求項15に記載の発明によれば、外部システムからバックアップ要求を受け付けた場合に、内部記憶媒体に格納した管理情報を所定の乱数により暗号化し、暗号化に用いた乱数を第1の暗号鍵により暗号化し、暗号化した暗号化管理情報および暗号化乱数をバックアップ情報として出力するよう構成したので、単に管理情報を暗号化するだけでなく、この暗号化に用いた乱数についても暗号化して出力することができる障害復旧方法が得られるという効果を奏する。

【0122】また、請求項16に記載の発明によれば、バックアップ情報に含まれる暗号化乱数を第1の復号鍵で復号化し、復号化した乱数で暗号化管理情報を復号化し、この復号化された管理情報を内部記憶媒体に記録するよう構成したので、暗号化された管理情報を正しく復号化して内部記憶媒体にリストアすることができる障害復旧方法が得られるという効果を奏する。

【0123】また、請求項17に記載の発明によれば、暗号化された暗号化管理情報に暗号化乱数を付与して暗号化内部情報を作成し、作成した暗号化内部情報のハッシュ値を算定し、算定したハッシュ値を暗号化内部情報とともにバックアップ情報として出力するよう構成した

ので、暗号化内部情報の改ざんを効率良く防止することができる障害復旧方法が得られるという効果を奏する。

【0124】また、請求項18に記載の発明によれば、バックアップ情報に含まれる暗号化内部情報のハッシュ値を算定し、算定したハッシュ値とバックアップ情報に含まれるハッシュ値とを比較し、両ハッシュ値が一致すると判断された場合に、暗号化乱数を第1の暗号鍵に対応する第1の復号鍵で復号化し、復号化した乱数を用いて暗号化管理情報を復号化するように構成したので、バックアップ情報が改ざんされているか否かを効率良く判断し、改ざんされていないことを条件として内部記憶媒体への管理情報の設定をおこなうことができる障害復旧方法が得られるという効果を奏する。

【0125】また、請求項19に記載の発明によれば、算定されたハッシュ値を第2の暗号鍵を用いて暗号化した暗号化ハッシュ値を暗号化内部情報とともにバックアップ情報として出力し、この第2の暗号鍵に対応する第2の復号鍵を用いて暗号化ハッシュ値を復号化したハッシュ値と算定されたハッシュ値とを比較するよう構成したので、暗号化ハッシュ値を用いてバックアップ情報の改ざんを防止することができる障害復旧方法が得られるという効果を奏する。

【0126】また、請求項20に記載の発明によれば、第1の暗号鍵および第2の復号鍵を公開鍵暗号系の公開鍵とし、第2の暗号鍵および第1の復号鍵を公開鍵暗号系の秘密鍵とするよう構成したので、公開鍵暗号系を用いてバックアップ情報の暗号強度を高めることができる障害復旧方法が得られるという効果を奏する。

【0127】また、請求項21に記載の発明にかかる記録媒体は、請求項11～20のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録し

たことで、そのプログラムが機械読み取り可能となり、これによって、請求項11～20の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図1】この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図2】図1に示した大容量記憶媒体に保持したファイル並びに内部記憶媒体に保持したファイルを説明するための説明図である。

10 【図3】図1に示した外部システムからの原本性保証電子保存装置へのログイン手順を示すフローチャートである。

【図4】図1に示したバックアップ処理部によるバックアップ手順を示すフローチャートである。

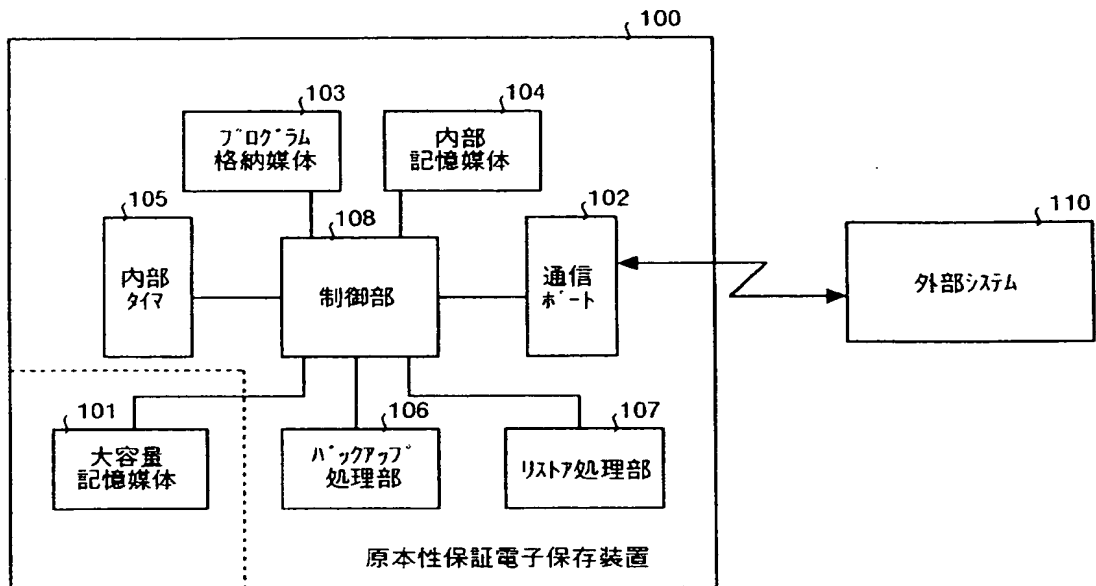
【図5】図1に示したリストア処理部によるリストア手順を示すフローチャートである。

20 【図6】図1に示したリストア処理部が、使用している原本性保証電子保存装置に相乗りする形で内部管理情報をリストアする場合のリストア手順を示すフローチャートである。

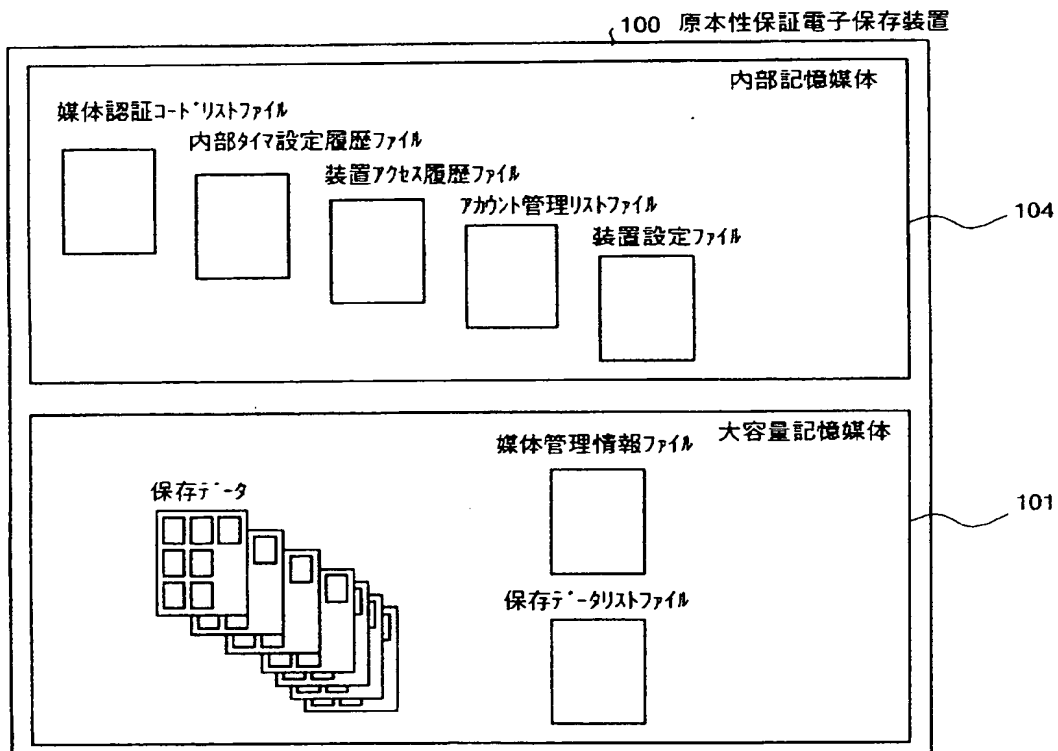
【符号の説明】

- 100 原本性保証電子保存装置
- 101 大容量記憶媒体
- 102 通信ポート
- 103 プログラム格納媒体
- 104 内部記録媒体
- 105 内部タイマ
- 106 バックアップ処理部
- 107 リストア処理部
- 108 制御部
- 110 外部システム

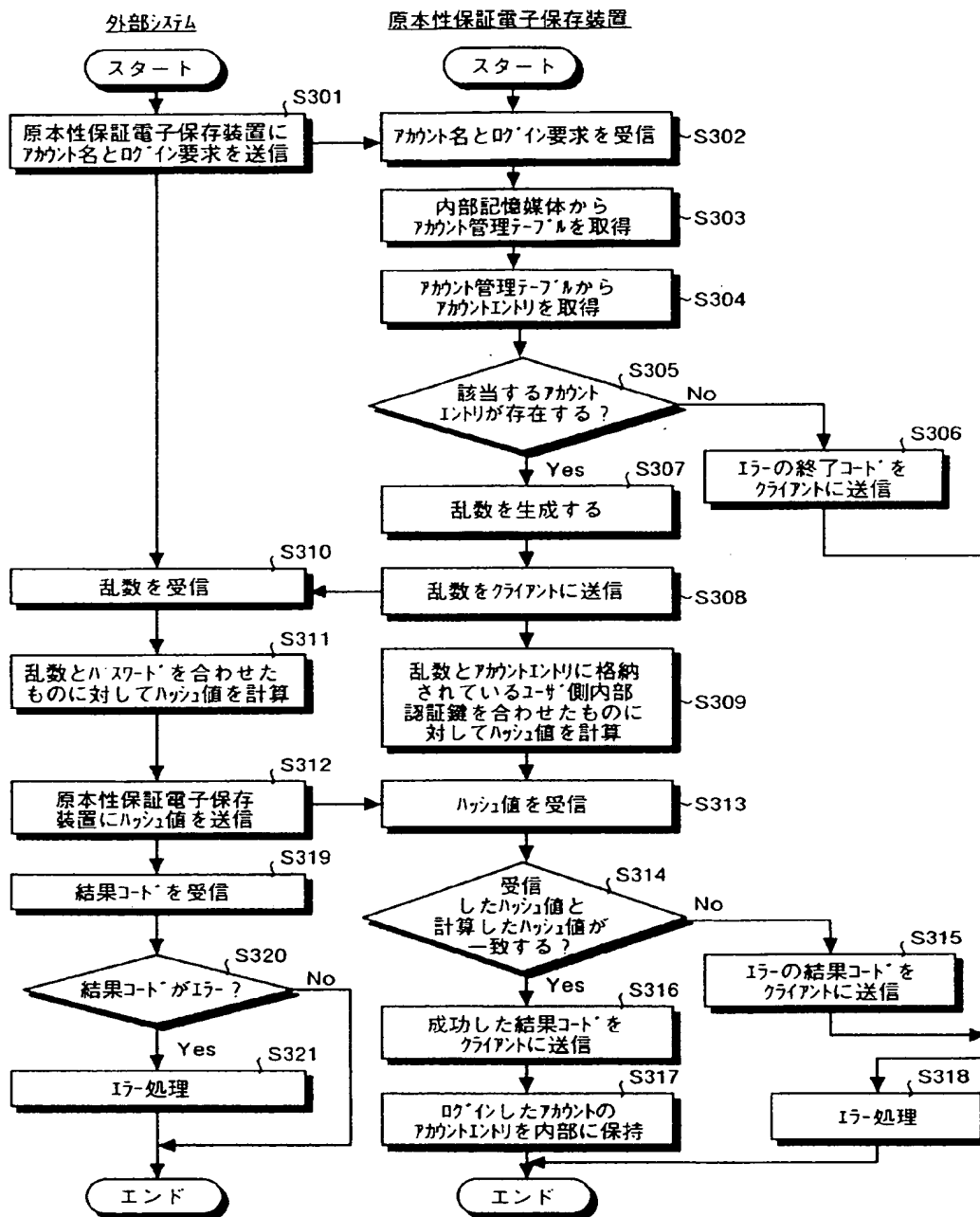
【図1】



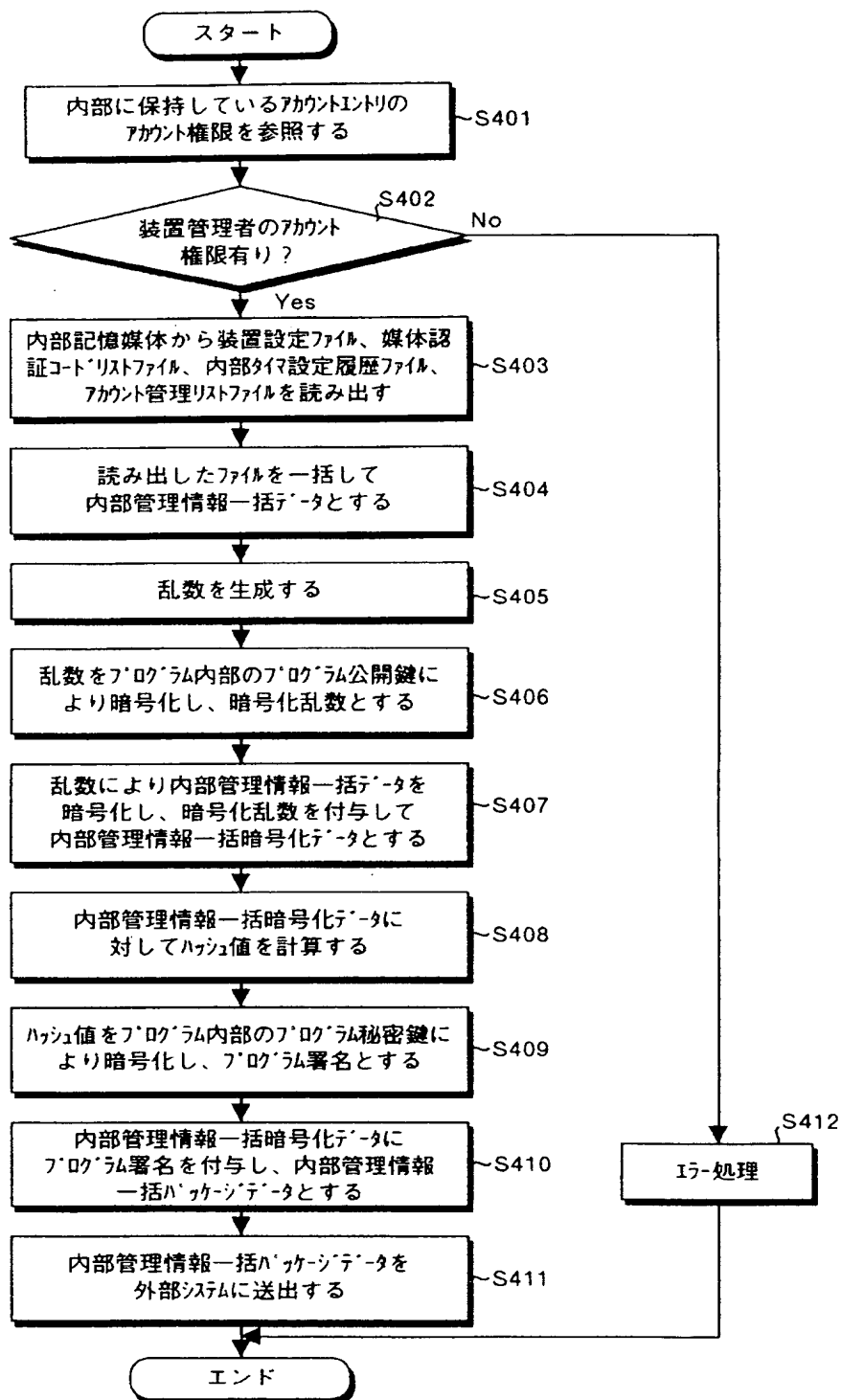
【図2】



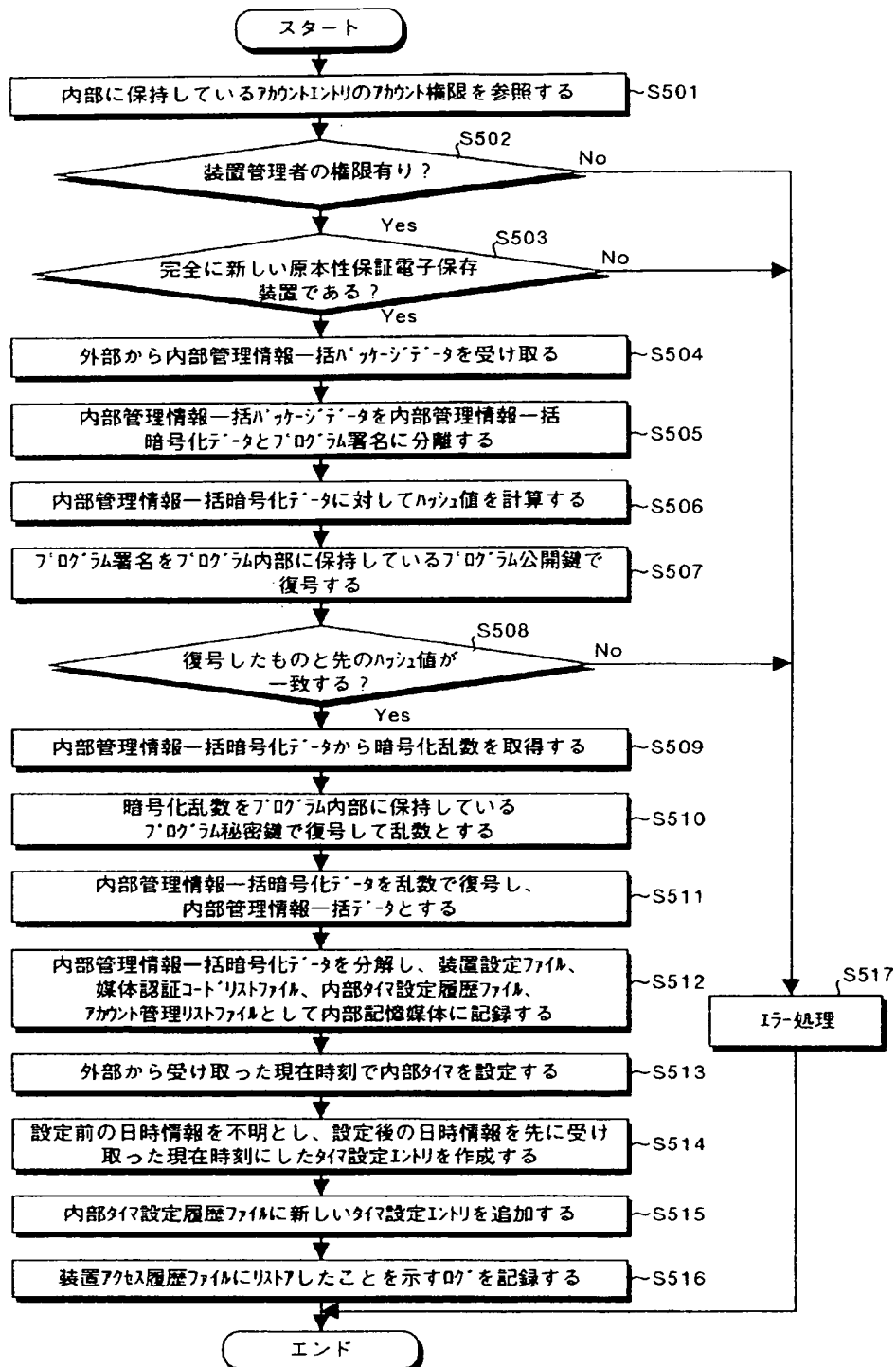
【図3】



【図4】



【図5】



【図6】

